EX PARTE OR LATE FILED

AVAYA

ORIGINAL

Charles E. Crowders
Vice President
Government Affairs
1212 New York Avenue, NW
Suite 1212
Washington, DC 20005
202-378-2374 voice
202-378-5798 fax
crowders@avaya.com

December 15, 2005

Marlene H. Dortch
Secretary
Federal Communications Commission
TW-A325
445 12th Street, SW
Washington, DC 20554

Re: Ex Parte Presentation – CALEA and Broadband Access – ET Docket No. 04-295

Dear Ms. Dortch:

Yesterday Dean Grayson, Don Price, David Ahrens, and I, all of Avaya Inc., met with Carol Simpson, Christi Shewman, Nick Alexander, Julius Knapp and Chris Killion, all of the FCC, to educate the FCC staff on Avaya and discuss several major areas included in the CALEA and Broadband Access NPRM. Specifically, Avaya urged the FCC to apply the CALEA statute's private network exception (47 USC 1002(b)(2)(B)) to certain scenarios involving virtual private networks. Avaya discussed what is technically possible today with regard to surveillance on VoIP communications, and what types of surveillance are made more difficult due to encryption technology – such as on phones operating with SIP protocol. Our discussion followed a "talking points" document that was provided to the FCC at the meeting, and is enclosed with this letter.

Please contact me at (202) 378-2374 with any questions.

Sincerely,

Charles Crowders/DLG

Charles E. Crowders
Vice President & Head, Government Affairs
Avaya Inc.

Talking Points for Avaya's Visit with the FCC

I. The Private Network Exception. The CALEA statute (47 USC 1002(b)(2)(B)) states: "The requirements of [CALEA] do not apply to equipment, facilities, or services that support the transport or switching of communications for *private networks* or for the sole purpose of interconnecting telecommunications carriers."

a) Avaya would like to confirm that the FCC's Order does not intend to alter or narrow the application of this exception for Private Networks.

b) Avaya interprets the FCC's Order (¶ 39 and footnote 100) to impose CALEA requirements on all VoIP communications that involve transmissions across either the PSTN or the Internet. However, in light of the statutory exception quoted above, CALEA does not apply to VoIP communications on networks that are *linked* to the PSTN or the Internet, but do not involve transmissions *across* either of those networks. For example, single-sited CPE-based business networks or firewalled, multi-sited large enterprises are still deemed private networks under the Private Network Exception provided that the communications are between in-network users, even though the network itself is connected to the Internet and permits parties to communicate with third parties outside of the Enterprise.

c) To the extent that individuals on those networks referenced in (b) initiate communications with out-of-network users, such traffic would be subject to CALEA at the Service Provider edge. If the CALEA surveillance takes place at the Enterprise, this would significantly jeopardize the goal of facilitating unobtrusive and undetected surveillance (e.g., 47 USC 1002(a)(4)) and greatly increase the cost of implementation.

d) Avaya interprets the FCC's Order to impose CALEA compliance requirements upon those networks that are used as extensions of a public network for communications between "public" users, for example Universities Student/Public Access LANs, or localized wireless networks (e.g. Coffee Shops LANs, or Internet Café LANs).

II. Encryption. Many VOIP protocols are incorporating encryption into their signaling (H235.5; SIP TLS) and media traffic (SRTP). Avaya is concerned about the impact of the FCC Order on products that include encryption as part of the product offering.

a) The goal of facilitating unobtrusive and undetected surveillance (e.g., 47 USC 1002(a)(4)) in an enterprise-based network becomes difficult to achieve if the encryption is end-to-end and the only access to un-encrypted traffic is via the manufacturer's equipment (i.e. there is no proxy or intermediary intelligent point

in the Service Providers network). In a scenario such as that described in Section V below, Avaya believes that CALEA would not apply unless the surveillance could be conducted at a point within the public network, and not at the actual user's phone or other communication device.

b) Avaya interprets CALEA and the FCC Order to require that surveillance be conducted by the PSTN or Internet Service Provider when communications traffic originates on an enterprise/ business network (i.e. the session is part of the routine execution of a private enterprise's means of communication and is not for the purposes of personal communication) and terminates in the public network

c) Avaya does not interpret CALEA to require that an Enterprise, or a Service Provider, change the normal routing of communications traffic to facilitate surveillance.

III. Definition of Information Services. The FCC Order (¶20-21) states that CALEA applies to certain traditional information services, such as the transmission of email. However, the Order makes further assertions as to when CALEA does, and does not apply regarding these information services.

a) Avaya offers products (Modular Messaging, UCC Speech Access) to facilitate secure, encrypted retrieval of voicemail and email, using a web browser (https). This information is retrieved from a customer's account within a private network. Avaya interprets this retrieval as falling within the rubric of "storage", which is excluded from CALEA. If the FCC disagrees, what definitions of "storage" and "redirection" is the Agency utilizing in paragraph 20 of the Order.

b) If the retrieval of voicemail and email (through the products referenced in (a) above) are covered by CALEA, then consideration must be given to the use of encryption in this process. While the communication from end to end is encrypted, law enforcement could intercept data either at the end point or at the server (or router or gateway) where the encrypted session keys are negotiated. While these session keys are utilized by the end point, law enforcement could perform surveillance at the server using these same keys.

IV. SIP Protocol. The SIP protocol supports a peer-to-peer architecture where two VoIP phones can negotiate security policy and establish encryption keys, and then communicate securely. Their communications traffic may or may not traverse public networks.

a) Avaya does not interpret the FCC's Order to apply CALEA to sessions where the users are both on the same private network, and therefore, no intermediary device is used to either perform encryption or carry the communications traffic.

b) Where one or both users are on public networks, use of the SIP Protocol would require law enforcement to obtain the TLS encryption keys at a server or router within the public network, rather than perform surveillance from the phone itself (or other appliance being used for the communication). Each phone sends signaling from one end-point to another. Recognizing the goal of facilitating unobtrusive and undetected surveillance (e.g., 47 USC 1002(a)(4)), Avaya believes that industry and law enforcement must establish a mutually agreed means of achieving appropriate surveillance before vendors such as Avaya are required to proceed with CALEA implementation.

c) How is CALEA applied to SIP peer-to-peer protocol usage (for example, either SKYPE or the open source PBX software entitled "Asterisk")? With this form of communication, a user utilizes the internet address of another party to communicate with that second party without involving hardware other than the two users' endpoints. No off-site server or media gateway intermediary equipment is necessary. Rather, the two communicating parties use a proprietary, non-standards-based protocol as well as encryption. In such a scenario, it would be virtually impossible to support CALEA without installing a surveillance device within the endpoint or otherwise modifying the nature of the endpoints themselves.

V. **Alternative communications method or network structures.**

a) Does CALEA cover instant messaging? Today, IM has the ability to transmit voice, data and messaging, even PowerPoint presentations. This technology has many characteristics of traditional email distribution. How does the FCC view this technology within the spectrum of communications?

b) Does CALEA apply to video in the same manner as any other communications media, following the same rules as those used for voice traffic?

c) Avaya believes that a "hosted" network should be treated the same as a "private network." In a hosted network, customers will acquire (through purchase, lease, or some other financial arrangement) either the possession or use of network equipment that is managed by another party, such as Avaya or a traditional service provider. Even if the customer does not hold legal title to its network equipment, that equipment has been specified by the customer, and is dedicated to the customer's use. Indeed, the managing party "hosts" the network as if it were the customer's secure private network. Avaya believes that where such a network sends communications traffic within the network itself, without utilizing the Internet or PSTN, such communication would be not subject to CALEA.